(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－127757
（P2001－127757A）
(43)公開日　平成13年５月11日(2001.5.11)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　12/22		Ｈ０４Ｈ　1/00	Ｆ	５Ｃ０６４
Ｈ０４Ｈ　1/00		Ｈ０４Ｌ　1/00	Ａ	５Ｊ１０４
Ｈ０４Ｌ　1/00		Ｈ０４Ｎ　7/16	Ａ	５Ｋ０１４
9/36		7/20	６３０	５Ｋ０３０
12/56		Ｈ０４Ｌ　11/26		

審査請求　未請求　請求項の数20　ＯＬ　（全 10 頁）　最終頁に続く

(21)出願番号　特願平11－307637

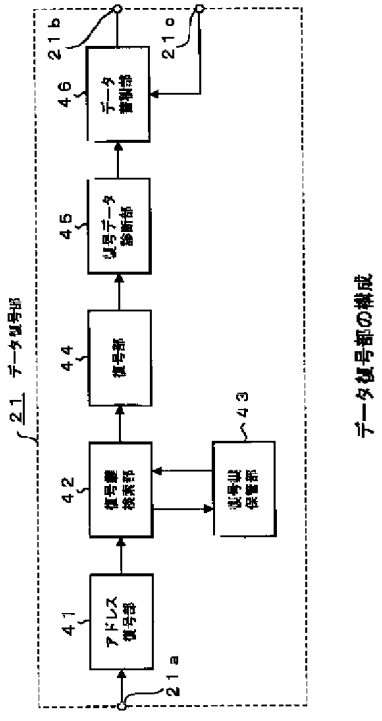
(22)出願日　平成11年10月28日(1999.10.28)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　石井　眞
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100080883
弁理士　松隈　秀盛

最終頁に続く

(54)【発明の名称】　データ受信方法及びデータ受信装置

(57)【要約】
【課題】　衛星伝送サービスなどにおいて、正しく復号されたデータのみを、接続されたホストコンピュータに転送できるようにする。
【解決手段】　受信したデジタル信号データの中から必要とするデータを取り出し、その取り出した受信データを所定の復号鍵により復号し、その復号されたデータの正誤を判定して正しく復号が行われていないデータであると判断したとき、該当する受信データを破棄するようにした。



データ復号部の構成

【特許請求の範囲】
【請求項１】　受信したデジタル信号データの中から必要とするデータを取り出し、その取り出した受信データを所定の復号鍵により復号し、
その復号されたデータの正誤を判定して正しく復号が行われていないデータであると判断したとき、該当する受信データを破棄するようにした、
データ受信方法。
【請求項２】　前記受信データは、コンピュータが扱うデータである、
請求項１記載のデータ受信方法。
【請求項３】　前記復号処理は、受信されるパケット毎に実時間で復号処理を行うようにした、
請求項２記載のデータ受信方法。
【請求項４】　前記復号されたデータの正誤判定処理は、受信されたパケット毎に復号が正常に行われたか否かを実時間で判断する処理である、
請求項３記載のデータ受信方法。
【請求項５】　前記受信データの破棄処理は、実時間で正しく復号が行われなかったデータを実時間で破棄する処理である、
請求項４記載のデータ受信方法。
【請求項６】　受信データに含まれるアドレスデータを判断し、自局宛のデータであると判断したとき、復号処理を実行するようにした、
請求項１記載のデータ受信方法。
【請求項７】　外部からの入力によって復号鍵を設定できるようにした、
請求項１記載のデータ受信方法。
【請求項８】　受信パケットの復号時に用いるべき鍵がない場合、当該パケットを破棄するようにした、
請求項１記載のデータ受信方法。
【請求項９】　前記復号鍵は、受信信号の送信側と同じ鍵を用いるようにした、
請求項１記載のデータ受信方法。
【請求項１０】　正しく復号が行われたと判断したデータだけを外部に出力するようにした、
請求項１記載のデータ受信方法。
【請求項１１】　受信手段と、
前記受信手段が受信した信号をデジタル信号に変換する変換手段と、
前記変換手段が変換したデジタル信号データの中から必要とするデータを取り出すデータ抽出手段と、
受信データを復号するために必要な復号鍵を設定するための復号鍵設定手段と、
受信したデータを前記復号鍵設定手段により設定された復号鍵を使用して復号する復号手段と、
前記復号手段で復号されたデータを検査する検査手段と、
前記検査手段で正しく復号が行われなかったと判断したデータを破棄する破棄手段とを備える、
データ受信装置。
【請求項１２】　前記受信手段が受信した信号に含まれるデータは、コンピュータが扱うデータである、
請求項１１記載のデータ受信装置。
【請求項１３】　前記復号手段は、受信されるパケット毎に実時間での復号が可能な手段である、
請求項１２記載のデータ受信装置。
【請求項１４】　前記検査手段は、受信されるパケット毎に復号が正常に行われたか否かを実時間で検査する手段である、
請求項１３記載のデータ受信装置。
【請求項１５】　前記破棄手段は、実時間で正しく復号が行われなかったデータを実時間で破棄する手段である、
請求項１４記載のデータ受信装置。
【請求項１６】　前記変換手段が変換した受信データに含まれるアドレスデータを判断し、自局宛のデータであると判断したとき、前記復号手段は復号を行うようにした、
請求項１１記載のデータ受信装置。
【請求項１７】　前記復号鍵設定手段は、外部からの入力によって復号鍵を設定できるようにした、
請求項１１記載のデータ受信装置。
【請求項１８】　前記復号手段でパケットの復号時に用いるべき鍵がない場合、前記破棄手段は当該パケットを破棄するようにした、
請求項１記載のデータ受信装置。
【請求項１９】　前記復号鍵設定手段により設定される復号鍵は、受信信号の送信側と同じ鍵を用いるようにした、
請求項１１記載のデータ受信装置。
【請求項２０】　前記検査手段で正しく復号が行われたと判断したデータだけを外部に出力する出力手段を備えた、
請求項１１記載のデータ受信装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、衛星データ配信もしくは通信サービスシステムで、例えば電子的に配信された個人向けのコンピュータデータを受信する際に適用して好適なデータ受信方法及びデータ受信装置に関する。
【０００２】
【従来の技術】ＭＰＥＧ２(Moving Picture Experts Group Phase2) は現行放送やＨＤＴＶ、ＡＶ機器などに適用される符号化方式であり、この符号化方式により符号化されたデジタル放送信号による放送サービスを行うことで、従来のアナログ放送に比べて多チャンネル化とチャンネル当たりのコストの削減をもたらし、映像・音声

のみならず各種データ放送等のサービスも可能である。
【０００３】これら多チャンネルディジタル放送においては、衛星の高速転送スピード（２７ＭＨｚトランスポンダの場合、最大３０Ｍｂｐｓ）を生かした各種のデータ放送が実施されている。データ放送には、例えば音楽サービス、ゲームサービス、雑誌情報サービス、インターネット（ＷＷＷ）サービスなどがある。
【０００４】データ配信サービスを通信衛星を用いて放送する際に、契約者のみ受信することが可能なシステムの提供は必要である。例えばデータ提供者が契約した人のみにデータを送信したい時、または受信側のユーザが、自分固有の秘密の情報をセンターから送信してもらいたい時、等の用途において、個人レベルの秘密保持機構が必ず必要になる。
【０００５】また、通信衛星によって、最速３０Ｍｂｐｓの高速データ転送を考慮した場合、受信側において受信中のデータを、実時間かつ高速に暗号化されたデータを復号しなければならない。
【０００６】さらには、衛星データ放送/通信サービス受信者が、一つの受信端末を用いて、本人のみ受信可能な秘密データを、複数種類（複数番組）を同時刻に受信するような状況がある場合、逐次実時間で変化する復号鍵を高速に検索及びスイッチしながら受信データを復号する様な機構が必要となる。
【０００７】
【発明が解決しようとする課題】このようなデータ放送サービスに使用される受信端末を考えた場合に、衛星データ受信のために必要な機能、受信した暗号データを実時間で復号する機能、復号のために必要な機能を実時間でスイッチングする機能等をすべて同一のハードウエアで効率よく行うことが重要となる。また、この様な、復号のために必要な復号鍵のスイッチング機能を高速で行うサービスの場合に、復号鍵の設定の方法によては、誤った復号鍵を復号部に設定してしまう恐れがある。復号鍵を誤って設定した際には復号は正しく行われず、まったくもって元のデータを復元することができなくなってしまう。しかし、受信したデータを、閲覧もしくは使用するコンピュータに誤ったデータを転送することはコンピュータの機構上許されない（最悪の場合にはコンピュータの破壊につながるため）。そこで、データ受信装置内で実時間でデータを復号する機構を持たせるためには、同時に、復号が正しく行われたかどうかを自己診断する機能は必要となる事が望ましいが、現状、その様な機構を持ち合わせたデータ受信システムは存在しない。
【０００８】本発明は、多チャンネル及び大容量衛星データ放送サービスや衛星インターネットサービスなどで受信する場合において、受信者が、受信者当人のみが受信可能な暗号化された大容量かつ多種類のデータを同時受信され、なおかつ、どんな状況化（鍵の設定誤りがサービスシステム的に発生する可能性がある）においても、正しく復号されたデータのみ受信して、ホストコンピュータに正しく復号されたデータのみを転送できるようにすることを目的とする。
【０００９】
【課題を解決するための手段】本発明のデータ受信方法は、受信したデジタル信号データの中から必要とするデータを取り出し、その取り出した受信データを所定の復号鍵により復号し、その復号されたデータの正誤を判定して正しく復号が行われていないデータであると判断したとき、該当する受信データを破棄するようにしたものである。
【００１０】また本発明のデータ受信装置は、受信手段が受信した信号をデジタル信号に変換する変換手段と、変換手段が変換したデジタル信号データの中から必要とするデータを取り出すデータ抽出手段と、受信データを復号するために必要な復号鍵を設定するための復号鍵設定手段と、受信したデータを復号鍵設定手段により設定された復号鍵を使用して復号する復号手段と、復号手段で復号されたデータを検査する検査手段と、検査手段で正しく復号が行われなかったと判断したデータを破棄する破棄手段とを備えるものである。
【００１１】本発明によれば、一人のユーザが本人のみ受信したい、もしくは送り手側がある特定のユーザにのみ配信したい機密性が高く大容量の衛星受信データの中で正しいデータのみを正確に、あるユーザが実時間で受信することが可能となる。また、復号後の診断を行うことにより何らかの理由により復号に失敗したデータを受信装置内で破棄する機構により、ホストコンピュータの負担の軽減やホストコンピュータの障害の軽減につながる。
【００１２】
【発明の実施の形態】以下、本発明の一実施の形態を、添付図面を参照して説明する。まず、本発明の受信装置が適用される衛星データ放送／通信サービスのシステム構成を、図１を参照して説明する。
【００１３】図１に示すように、衛星データ放送／通信サービスは、複数の情報提供者１ａ～１ｎと、その情報提供者１ａ～１ｎの情報を放送データとして通信衛星３に送出するサービス運用会社２で構成され、通信衛星３で中継された放送データを、各契約者４ａ～４ｎに設置された受信装置で受信する。この場合、各契約者４ａ～４ｎとサービス運用会社２との間は、公衆電話回線，専用回線などの有線伝送路５で接続される構成としてあり、各契約者からサービス運用会社２に情報を送ることができる構成としてある。また、サービス運用会社２は、インターネット６と接続してあり、任意のインターネット情報を通信衛星３を介して伝送できるようにしてある。
【００１４】各契約者４ａ～４ｎは、サービス運用会社２が取りまとめて送信する、例えば新聞情報、雑誌情

報、音楽情報、ショッピング情報、インターネットＷＷＷ情報等のコンピュータで閲覧及び操作可能な情報を得るために、サービス運用会社２と契約を結ぶ。サービス運用会社２は、各情報提供者１ａ～１ｎが取り扱い及び発信する様々な情報を取りまとめ、通信衛星３に情報を打ち上げる。ここでサービス運用会社２は、通信衛星３にデータを打ち上げる際に、衛星通信路上のデータフォーマットは、サービス運用会社２の自由なフォーマットで打ち上げるのではなく、欧州や日本等の現行で運営されている衛星放送と同様なデータフォーマットであるＤＶＢ規格等の標準規格に準じたフォーマットに変換して打ち上げることが前提となる。

【００１５】一方、サービス運用会社２と契約した契約者４ａ～４ｎは、契約時にサービス運用会社２が提供する受信アンテナと受信装置を用いることによって、サービス運用会社２から通信衛星３を経由して配信されるデータを受信することが可能となる。

【００１６】ここでの受信装置は、例えば現行のＢＳ放送やＣＳ放送等で放映されている、映像や音声サービスのみならず、コンピュータで扱える情報を受信することを目的とした受信装置であり、現在一般的に普及されているコンピュータに内蔵するボードタイプもしくはコンピュータにデータ転送することが可能なボックスタイプ（セットトップボックス）で構成される。

【００１７】従って、各契約者は、受信アンテナからの同軸ケーブルを、コンピュータ内蔵の受信データ装置（ボード）に直接接続するか、もしくはボックスタイプのデータ受信装置に接続してデータを受信する使用することになる。また、図１に示す衛星データ放送／通信サービスは、サービス運用会社２からの、例えば現行のＢＳ放送またはＣＳ放送の様な一方向的な映像サービス、音声サービスを契約者に配信するだけではなく、インターネットのWWW情報閲覧の様な、契約者の一人がある時刻で要求する情報に応じてその情報を通信衛星３で配信する様なインタラクティブなサービスも対象となる。従って、ある時刻における通信衛星路上には、例えば現行のテレビ放送の様に全ての契約者が同時に見える情報を送信されているだけでなく、特定の契約者一人のためだけの情報が送信されていることが起こり得る。

【００１８】この様な場合に備えて、通信衛星３からの情報の元の信号自体は契約者全員が受信可能であるが、その中で、ある特定の契約者が個人で（もしくは団体で）契約した情報のみしか見ることができない機構が必要となる。すなわち、例えば特定の契約者４ａがサービス運用会社２に有線伝送路５を介してリクエストした情報は、通信衛星路を通って、その情報の元の信号自体を他の契約者４ｂ～４ｎが受信することは可能であるが、意味ある情報として得られるのは契約者４ａだけであり、契約者４ｂ～４ｎは契約者４ａ用に配信された情報は永久に意味ある情報として得ることができないという機構である。本発明によるデータ受信装置は、この機構を備えるものである。

【００１９】また、各契約者が、ある任意の時刻に、インターネット６のWWW情報閲覧の様な、自分だけのための情報が欲しいと判断した際に、データ受信装置を内蔵するコンピュータが保有するモデムやEtherNetのインターフェースにより例えば公衆回線網または専用線等の有線通信路を経由して、情報のリクエスト命令をサービス運用会社２に発信する。特定の契約者からの特定の情報のリクエストを受けたサービス運用会社２は、情報の種別によってインターネット６にアクセスもしくは、情報提供者１にアクセスして契約者からの特定のリクエストの情報を得る。そして、サービス運用会社は、得た特定の情報をその契約者しか受信できない形態に情報を変換（暗号化）して通信衛星３にデータを打ち上げる。そして、その要求を行った特定の契約者は、送信側から送られてくる自分宛てだけのために（他の契約者が受信することができように）暗号化されたデータを、元々自分のみ保持しているはずの復号鍵を用いて復号することによって自分だけが必要とするデータを受信する事が可能となる。

【００２０】以上が、本発明によるデータ受信装置を使用する衛星データ放送／通信サービスのシステムの概要である。

【００２１】次に、以上説明したシステムに適用される本発明のデータ受信装置の構成について、図２及び図３を参照して説明する。まず、衛星通信路上のデータを受信するデータ受信装置の全体構成を、図２を参照して説明する。

【００２２】衛星通信路上の全データは、受信アンテナ１１で受信し、受信アンテ１１からの信号を、同軸ケーブ１２を介してデータ受信装置２０に供給する。データ受信装置２０は、同軸ケーブル１２の入力端子を備えており、そこから受信ＩＦ信号が入力される。

【００２３】ここでの受信ＩＦ信号には、ある契約者が欲しい特定の情報以外の情報も全て（データ受信端末用の制御情報や、他契約者宛ての情報も含む）入っている。受信された受信ＩＦ信号は、衛星データ取り込み部２１によって、特定の受信チャンネルの受信信号をデジタルデータに変換するＡＤ変換や、データの同期取り、パケット化等が行われる。

【００２４】衛星データ取り込み部２１によってデジタル化された受信パケットは、データ復号装置２２にて復号処理が行われる。ここでは、受信パケット内のＭＡＣ（MediaAccessController）ヘッダ内のＭＡＣアドレス（宛先アドレス）と、この受信装置の制御部２４によって指定されたＭＡＣアドレス（即ち自局に設定されたアドレス）を比較し、一致した場合かつそのパケットが暗号化されている場合に、復号処理が行われる。制御部２４内にパケット内に存在するＭＡＣアドレスと同等のア

ドレス値が存在する場合に、「復号すべき復号鍵が存在する」ということを意味し、予めそのＭＡＣアドレスと対になって設定されている復号鍵を用いてパケットを復号する。

【００２５】なお、受信パケットの構成としては、例えば図４に示すように、ＭＡＣヘッダ内には、ＭＡＣアドレス（宛先アドレス）以外に、暗号化有無情報（そのパケットが暗号化されているかいないかという情報）も入っており、暗号化されている情報が有効を示した場合のみ復号を行い、暗号化されているという情報が無効を示していた場合にはパケットを復号せずに、パケットを受信データ出力インターフェース２３に直接転送する構成としてある。

【００２６】また、衛星データ取り込み部２１からデータ復号部２２に入力されたパケット内のＭＡＣアドレスと制御部２４により指定されたＭＡＣアドレスが一致してなく、かつ、パケットのＭＡＣヘッダ内の暗号化情報が有効となっていた時（即ち暗号化されているとき）、それは「パケットが暗号化されているため復号しなければならないが、復号のための鍵が存在しない」ということを意味して、その場でそのストリームを破棄する。

【００２７】復号するための鍵が正常に存在して、なおかつデータ復号部２２によって復号されたパケットはその後、同装置内にて正常にパケットが復号されたかどうかの診断が行われ、もし復号が正常に行われてたことが診断されたという結果になった場合のみ、その後段である受信データ出力インターフェース２３にパケットが転送される。もしこの時データ復号部２２内にてパケットの復号後の診断にて「パケットは復号されたが、復号は正常に行われなかった」という結果になった場合は、そのパケットは受信データ出力インターフェース２３に転送されずに破棄される。

【００２８】ここで、データ復号部２２内にて行われる「復号されたパケットが正常に復号されたかどうかを診断」する処理について述べる。通信衛星から伝送されるパケットは、大まかには図４に示すパケットフォーマットになっている。ＭＡＣアドレスや暗号化有無情報等が格納されているＭＡＣヘッダの後に、実際に伝送されるデータ（コンピュータ用のデータなど）が配置されるペイロード部がある。暗号化されるのはこのペイロード部以降であり、ＭＡＣヘッダは暗号化されない。また、暗号化されたペイロードの後に復号診断コードがあらかじめ入っている。この復号診断コードの中身は何でもよいが、送信システム、受信システム間で定められた一定の定数値としてある。

【００２９】復号診断コードもペイロード部と同等の暗号鍵によって暗号されており、もしデータ復号部が正しい復号鍵を用いて復号を行った場合に、必ず復号後の復号診断コードの値は、送信システム側と受信システム側の両方で予め決められた一定の値になるはずである。また、もし誤った復号鍵によって復号された場合に、復号診断コードは予期せぬ値となり、ペイロード部も含めて復号が失敗したことが分かる。以上が、復号診断の基本的な仕組みである。

【００３０】受信データ出力インターフェース２３は、正常に復号できたデータパケットを例えばＬＡＮ等で接続されているホストコンピュータ３０に転送する。この時に受信データ出力インターフェース２３は、ＬＡＮ等で接続されているホストコンピュータとの通信プロトコルを守るロジックを持っていることが前提となる。

【００３１】また制御部２４は、データ受信装置全体を監視及び管理する。具体的には、データ受信装置と接続されるホストコンピュータ３０のアプリケーションからの制御命令や、通信衛星からの受信データの中に入っているデータ受信装置を制御するためのデータを解釈して、データ受信装置全体の監視及び管理を行う。ホストコンピュータ３０からのアプリケーションからの制御命令は、例えばＬＡＮ等の通信路経由で受信データ出力インターフェース２３から受け取る。

【００３２】データ復号部２２によってパケットの復号に用いられる復号鍵は刻々と変化することがあり、その度に制御部２４によって復号鍵が渡される。また、制御部２４に刻々と変化する復号鍵を設定するのはホストコンピュータ３０である場合もある。ここで、刻々と変化する復号鍵を制御部２４が正しく設定しなければ、データ復号部２２が復号時に使用する復号鍵は誤ったものとなる。

【００３３】どのような時に、データ復号部２２に設定されるべく復号鍵が誤ったものになるか、の例を説明する。通常、自分のアドレスを示すＭＡＣアドレスは、あるサービスにおいて長時間同一の物を使用する。しかし、長時間ある契約者が同一ＭＡＣアドレスを使用していても、復号鍵を随時変更することによってハッカーからの盗聴防止を行う事ができる。（すなわち、同一ＭＡＣアドレスのパケットに対して時刻毎に復号に用いる鍵が変化していく。）データ復号部２２内で誤った復号鍵を用いる可能性の高いのは、あるＭＡＣアドレスに用いられていた復号鍵がある時刻によって新しい復号鍵（ＭＡＣアドレスは同一）に切り替わった瞬間である。

【００３４】送信システム側ではあるＭＡＣアドレスに対して新しい暗号鍵を用いて暗号してデータ伝送しているのに関わらず、データ受信装置内のデータ復号部２２、もしくは制御部２４内にはあるＭＡＣアドレスに対して古い復号鍵が残っていた場合に（まだ新しい鍵に切り替わる直前）誤った復号鍵による復号が行われ、データは正しく復元されない。この様な場合がもっとも誤った復号鍵を用いて復号してしまう可能性が高い例である。（もちろん他にも誤った復号鍵の使用例は考えられるがここでは省略する）

【００３５】また、誤った復号鍵によって復号された無

意味なパケット、もしくは何らかの理由で復号が正常に行われなかった無意味なパケットがもしホストコンピュータ３０に転送された場合に、ホストコンピュータ３０内で破棄しなければならなくなる。

【００３６】ここで、データ受信装置内で復号失敗パケットを破棄する事は、ホストコンピュータ３０の負荷の低減および、無意味なパケットを正常なパケットのふりをしてホストコンピュータ３０に転送した場合に、最悪の事態としてホストコンピュータ３０が破損する可能性も出てくるのでその状態を防ぐ、という２点で非常に重要である。

【００３７】次に、本例の受信装置内のデータ復号部の構成及び処理について説明する。本例の復号部は、図３に示すように構成される。即ち、衛星データ取り込み部２１から端子２１に供給される受信データは、アドレス復号部４１でＭＡＣヘッダ内のアドレスデータが復号されて、その復号されたアドレスが、自局に設定されたアドレスと一致したとき、そのパケットのデータを、復号鍵検索部４２に供給する。アドレスが一致しない受信パケットについては、自局宛のデータでないと判断して破棄し、後段の処理系に供給しない。

【００３８】復号鍵検索部４２では、復号鍵保管部４３に保管された復号鍵の中から、このとき復号に使用する鍵を得る要求を行い、その要求で得た復号鍵のデータを、受信パケットと共に復号部４４に供給する。

【００３９】復号部４４では、その供給された受信パケットデータを、復号鍵を使用して復号処理を行い、暗号化されたデータの復号処理を行う。そして、復号部４４で復号されたデータは、復号データ診断部４５に供給し、この診断部４５で、各パケットに付加された復号診断コード（図４参照）の値を判断し、その値が予め決められた一定値であるか否か判断する。ここで、一定値でないパケットの受信データについては、この診断部４５でそのパケット全体を破棄し、一定値となったパケットのペイロード部の復号データだけを、データ蓄積部４６に供給する。データ蓄積部４６は、一時的にデータを蓄積する比較的小容量のメモリで構成したり、或いはハードディスク装置などの大容量記憶装置を使用しても良い。このデータ蓄積部４６に蓄積されたデータは、受信データ出力インターフェース２３から端子２１ｃを介して供給される転送要求に応じて、端子２１ｂから受信データ出力インターフェース２３に逐次転送し、このインターフェース２３から接続されたホストコンピュータ３０に受信データを転送する。

【００４０】ここで、このデータ復号部２１を構成する各部をより詳細に説明すると、以下のようになる。

【００４１】・復号鍵検索部４２

受信データ取り込み部２１より受け取ったパケットのＭＡＣヘッダ内のＭＡＣアドレスと予め制御部２４により設定されているＭＡＣアドレスが一致しているかどうかを比較し、もし一致していたら、そのＭＡＣアドレスに対応する復号鍵（ＭＡＣアドレスと復号鍵はある時刻において必ず対となって復号鍵保管部４３内に保存されているはずである）を復号鍵保管部４３より読み出してくる。

【００４２】復号鍵保管部４３より読み出されたあるＭＡＣアドレスに対応する復号鍵は、受信中のパケットデータ全体と共に、次の復号部４４に転送される。（なお、この時同じに復号部４４に「復号命令」も出す）

【００４３】もし、受信データ取り込み部２１より受け取ったパケット内のＭＡＣヘッダ内のＭＡＣアドレスと一致するアドレスが全体制御部２４より設定されていない場合は、「復号すべき鍵が存在しない」ということになり、このブロックの中でパケット全体が破棄される（すなわち次の復号部４４に転送されない）。

【００４４】なお、この処理は、受信データ取り込み部２１より受け取ったパケットのＭＡＣヘッダ内の暗号化有無情報が暗号されていることを示していた場合のみの処理である。もし、受信したパケット内の暗号化有無情報が「暗号されていない」ことを示していた場合、ＭＡＣアドレスの比較はせずにそのままパケットは次の復号部４４に転送される。（もちろん、その時復号部４４に対して「復号命令」を出さずにそのまま通過するように指示を出す）

【００４５】また、ある時刻において、復号可能となる復号鍵の数は１つに限らない。（すなわち、複数の復号すべきパケットのＭＡＣアドレスがこのブロック内に制御部２４より設定されいていることもありえる。）

【００４６】・復号鍵保管部４３

この復号鍵保管部４３内に、ある時刻において有効となる、ＭＡＣアドレスと復号鍵の対が複数格納されている。ある時刻において有効なＭＡＣアドレスと復号鍵の対は、制御部２４によって随時設定される。ある時刻においてこのブロック内に存在するＭＡＣアドレスの値は、復号鍵検索部４２内に設定されているＭＡＣアドレスの数と値は、まったく同一のものである。（制御部２４は、復号鍵検索部４２と復号鍵保管部４３の両ブロックに対して、同時刻に同一の値を設定する必要がある）

【００４７】また、サービスの内容によって、全てのパケットが暗号化されいない状況があった場合には、復号鍵保管部４３内には、ＭＡＣアドレスと復号鍵の対はまったく存在しないことになる。

【００４８】復号部４４

復号鍵検索部４２から受け取った復号鍵を用いて、同時に受け取った暗号データパケットを復号する。この時、復号鍵検索部４２より「復号命令」も同時に受けることが前提となる。もし、「復号命令」を受け取らなかった場合には、復号鍵を無視して、受け取ったパケットはそのまま復号せずに通過させる。ここでの暗復号は基本的に「秘密鍵暗号方式」とする。復号部４４で復号後、復

号データ診断部４５へは、「復号命令」を受けた時の復号されたパケットもしくは、「復号命令」を受けなかった時のそのまま通過させたパケットの２種類である。（復号鍵は転送されずにこのブロック内で破棄され、次のパケットの入力を待つ。）

【００４９】・復号データ診断部４５

復号部４４より転送されたパケットが「正しく復号されたかどうか」を診断するブロックである。本ブロック内にて、「正常に復号された」　と診断された場合のみ、次のデータ一時蓄積部４６にパケットが転送され、もし「正常に復号されていない」という診断された場合には、本ブロック内にてパケットは破棄される。

【００５０】本ブロックにおける「パケットが正しく復号されたかどうか」の診断処理は、前述の通り、パケット内の最後に付随されている復号診断コードが予め送信システムと受信システムで決められた定数を示しているかどうかによって診断される。すなわち、送信システム側で、ある定数としてパケットの最後に付加した復号診断コードをパケットのペイロード部を暗号する鍵と同じ鍵を用いて暗号するため、データ受信装置内にて正しい鍵を用いて正しく復号された場合には必ず復号診断コードは再現されるはずである。（もし、正しく復号されていない場合には、復号診断コード30は予期せぬ値となり、すなわちそれはそのパケット全体が正しく復号できていない　ということを示すことになる。）

【００５１】また、もともと送信側によって暗号化されていなく、復号部４４を通過してきたパケットは、復号診断コードは正しい値が入っているはずであり、本ブロックにおいてパケットが破棄されることはない。

【００５２】なお、ここで診断部４５によって破棄されるパケットは（前述の通り）以下のパケットである。

・あるＭＡＣアドレスに対する復号鍵は間違って設定されていた場合。これは送信側であるＭＡＣアドレスに対する暗号鍵が刻々と変化していくために、データ受信装置内において刻々と変化していく復号鍵の設定が間に合わない際に起こり得る。もしくは制御部２４による復号鍵の設定失敗によって起こり得る。

・復号部４４によって何らかの処理エラーが発生した場合

【００５３】また、データ受信装置内で復号後診断を行わなければならない理由は（前述の通り）以下である。

・復号に失敗した無意味なパケットをホストコンピュータに転送することにより、ホストコンピュータ内で無意味なパケットを破棄しなければならないため、ホストコンピュータの負担増大となるため、無意味なパケットはホストコンピュータに転送すべきではない。

・復号に失敗した無意味なパケットをホストコンピュータに転送することにより、ホストコンピュータ27に障害（最悪の場合は破壊）につながる可能性があるため、無意味なパケットをホストコンピュータに転送すべきではない。

【００５４】・データ一時蓄積部４６

復号データ診断部４５から転送された「正しく復号されたパケット」もしくは「もともと暗号化されていないパケット」が本ブロックに蓄積される。このブロックは、最終的にパケット転送する先であるデータ受信装置外部のホストコンピュータ３０と何らかの方法によって接続される受信データ出力インターフェース２３間のデータ転送プロトコル（例えばＴＣＰ／ＩＰ）の通信都合によって発生する時間的な遅延を吸収するための役割を持つ。データ一時蓄積部４６は、受信データ出力インターフェース２３からのデータパケット要求によって初めてデータパケットを転送する仕組みとなっているため、データを一時的に蓄積する必要がある。

【００５５】ここで、このデータ復号部２１での処理を、フローチャートに示すと、図５に示すようになる。即ち、必要とする帯域の信号を受信し（ステップ１０１）、その受信データに含まれるアドレスが自局宛のアドレスであるか否か判断し（ステップ１０２）、自局宛のアドレスでない場合には、暗号化されたデータの復号処理を中止する（ステップ１０３）。なお、自局宛のアドレスでない場合でも、各局で共通に受信できるようなデータである場合には、復号処理を行う。

【００５６】そして、アドレスの一致などで受信が可能なデータであると判断したとき、その受信パケットが暗号化されているか否か判断し（ステップ１０４）、暗号化されている場合に、正しいと思われる復号鍵を使用して復号処理を行い（ステップ１０５）、その復号されたパケットのデータが正しいデータであるか否か判断する（ステップ１０６）。ここで、正しく復号されたデータであると判断されたとき、そのデータを一時蓄積部４６に転送し（ステップ１０７）、その蓄積されたデータを所定の転送要求に基づいて出力させる（ステップ１０８）。また、ステップ１０６で正しいデータでないと判断したとき、そのパケットのデータを全て破棄する（ステップ１０９）。また、ステップ１０４で暗号化されてない受信データであると判断したとき、復号せずに直接蓄積部に供給した後、出力させる。

【００５７】なお、上述した実施の形態に示したデータ受信装置は、コンピュータ内蔵タイプではなく、ボックスタイプとした例としたが、コンピュータ内蔵タイプなど種々の形態の受信装置として構成できるものである。また、上述した実施の形態では、衛星通信を利用してデータを受信するシステムに適用したが、他の伝送路を使用してデータを受信するシステムにも適用できることは勿論である。

【００５８】

【発明の効果】以上説明したように、本発明によると、一人のユーザが本人のみ受信したい、もしくは送り手側がある特定のユーザにのみ配信したい機密性が高く大容

量で多種類の衛星受信データをあるユーザが実時間で同時に受信することが可能となる。この場合、正しく復号処理が行われたかどうかを診断して誤ったデータを破棄する機構を内部に持つため、誤って復号されたデータが接続されたコンピュータ側に転送されることがなく、コンピュータ側で誤ったデータによる誤動作が発生することがなく、ユーザが使用するコンピュータの負荷の軽減、もしくはコンピュータの障害発生の減少に役立つ。

【図面の簡単な説明】

【図１】本発明の一実施の形態が適用される衛星データ放送／通信サービスのシステム構成例を示した構成図である。

【図２】本発明の一実施の形態によるデータ受信装置の全体構成を示したブロック図である。

【図３】本発明の一実施の形態によるデータ受信装置のデータ復号部の詳細を示すブロック図である。

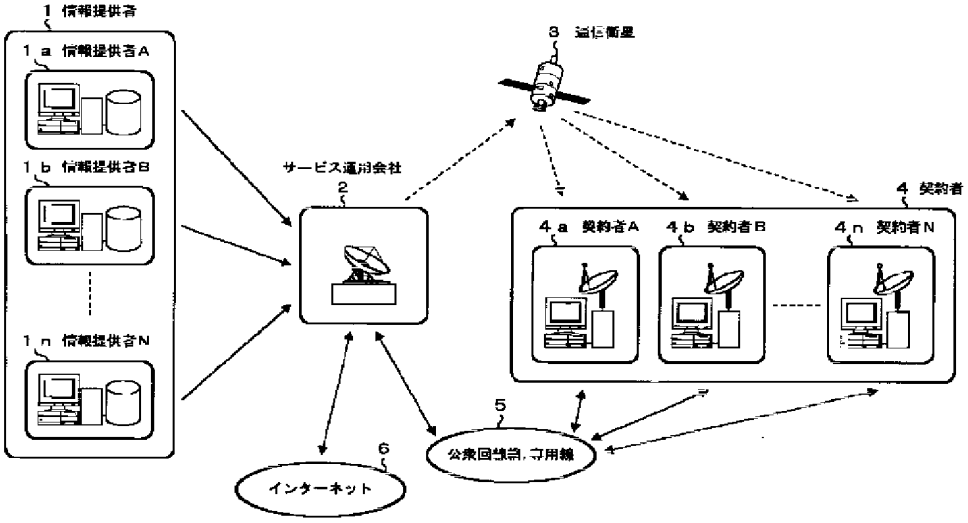
【図４】本発明による衛星データ放送／通信サービス用伝送路上のパケットフォーマット例を示した説明図である。

【図５】本発明の一実施の形態による復号部での処理例を示すフローチャートである。

【符号の説明】

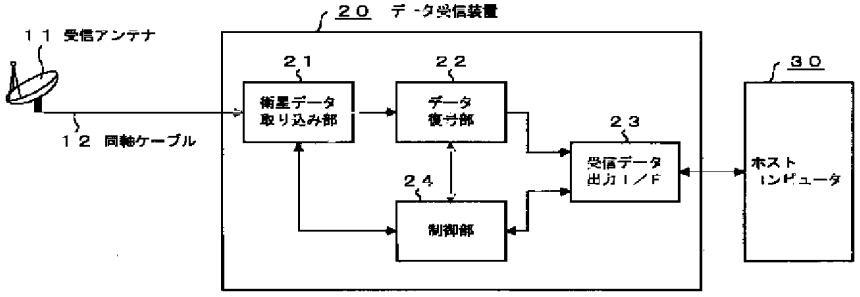
１ａ～１ｎ…衛星データ／通信サービスにおける情報提供者、２…サービス運用会社、３…通信衛星、４ａ～４ｎ…契約者、５…有線伝送路、６…インターネット、１１…受信アンテナ、１２…同軸ケーブル、２０…データ受信装置、２１…衛星データ取り込み部、２２…データ復号部、２３…受信データ出力インターフェース、２４…制御部、３０…ホストコンピュータ、４１…アドレス復号部、４２…復号鍵検索部、４３…復号鍵保管部、４４…復号部、４５…復号データ診断部、４６…データ蓄積部

【図１】



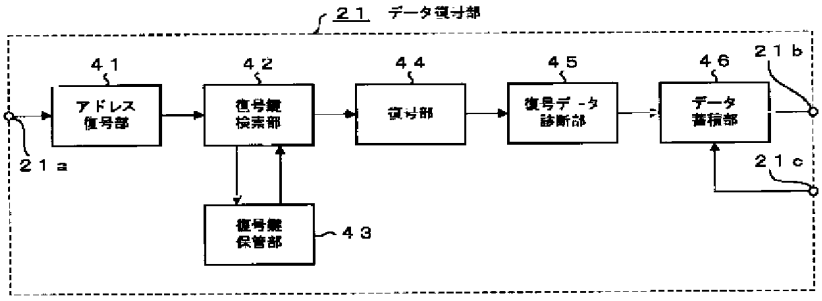
衛星データ放送／通信サービスのシステム構成例

【図２】



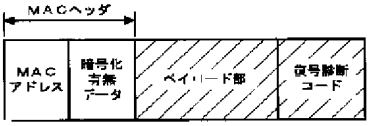
データ受信装置の構成例

【図３】



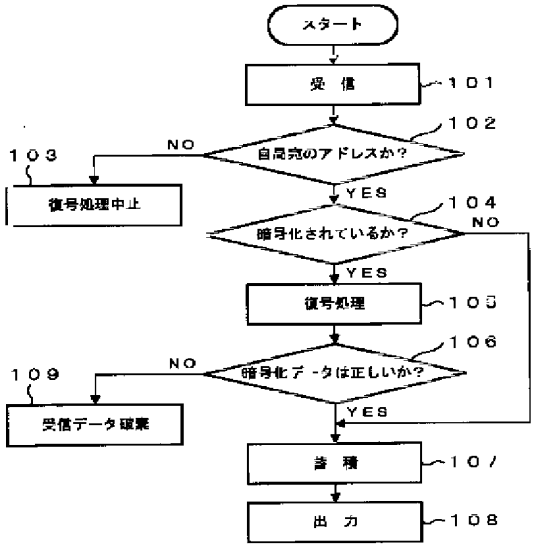
データ復号部の構成

【図４】



衛星データ放送／通信サービス用
伝送路上のパケットフォーマット

【図５】



データ復号部での処理例

フロントページの続き

(51)Int.Cl.⁷		識別記号	FI		(参考)
H04N	7/16		H04L	9/00	685
	7/167			11/20	102Z
	7/20	630	H04N	7/167	Z

Fターム(参考) 5C064 BA01 BB05 BC22 BD13 CC04
DA12
5J104 AA01 AA07 AA28 BA03 BA04
KA02 KA04 NA02 NA05 PA04
PA05 PA09
5K014 AA01 EA06 FA00
5K030 GA15 HC01 JL02 LA01 LC15
LC18 LD07